Stratton VA Medical Center
IRB Standard Operating Procedure: Privacy of Research Subjects & Confidentiality of Data

In order to approve research, the IRB, which includes the Information Security and Privacy Officers (ISO/PO) as non-voting ex-officio members, determines whether there are adequate provisions to protect the privacy interests of research subjects and the confidentiality of data both during and after their involvement in research. These provisions must be in accordance with the regulatory and guidance criteria provided by 38 CFR 17.33(a), .33(f), .278, and .500-.511, VHA Directive 2007-040, VHA Handbook 1605.1, VA IT Directive 06-2, and VA Directive 6504.

This standard operating procedure (SOP) has been prepared to assure compliance with the requirements of Standards for Privacy of Individually-Identifiable Health Information (HIPAA Privacy Rule), 45 CFR Parts 160 and 164, and other laws regarding protection and use of veterans' information, including Privacy Act of 1974, 5 U.S.C. 552a; VA Claims Confidentiality Statute, 38 U.S.C. 5701; Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Infection with Human Immunodeficiency Virus (HIV), and Sickle Cell Anemia Medical Records, 38 USC 7332; and Confidentiality of Healthcare Quality Assurance Review Records, 38 USC 5705. Research information that includes PHI shall be stored, maintained, and accessed in a manner that ensures that subjects privacy and confidentiality of their data is maintained in accordance with the policies outlined in VA Directive 6504.

A Health Insurance Portability and Accountability Act (HIPAA) Authorization request for the use and or disclosure of Protected Health Information (PHI) must be discussed with subjects as part of the informed consent process. IRB approval is required for the HIPAA Authorization form that must be signed by the subject. A HIPAA Authorization form with the IRB date stamp must be used. The IRB approval of the HIPAA form is considered during the review of the application to conduct research.

Obtaining HIPAA Authorization may be waived by the IRB, based on the HIPAA Privacy Rule regulations which stipulate that a waiver may be given when all four of the following items are met:

1) No more than minimal risk to privacy based on, at least, a:
   a) Written plan to protect identifiers
   b) Written plan to destroy identifiers as soon as possible
   c) Written assurance to the IRB that the PHI will not be re-used or disclosed except:
      i) As required by law
      ii) For authorized oversight of the research
      iii) For other research that has been reviewed and approved by the IRB with specific approval regarding access to the PHI

2) Research cannot practicably be done without the waiver
3) Research cannot be done without the PHI
4) Uses and disclosures of PHI must be limited to the minimum necessary to achieve the research purpose

The decision to grant a waiver from obtaining HIPAA Authorization and the justification must be fully documented in the minutes of the IRB meeting where the action was taken or reported (if approved by expedited review). [VHA Handbook 1200.5 7.a (4) (b)]

VA personnel may obtain and use medical, technical, and administrative records from this or other VA facilities for research purposes. VA employees at this facility may obtain PHI under the following circumstances.

1. When HIPAA Authorization is provided by the subject.
2. When a Waiver Of Authorization is approved by the IRB (No HIPAA Authorization is required)
3. When the activity is Preparatory to Research (No HIPAA Authorization is required)
4. When the research involves a limited data set or de-identified health information (No HIPAA Authorization is required)

Obtaining and using medical, technical, and administrative records from other VA facilities or VA databases (national, regional, or subject specific) for R&D purposes must be in compliance with all VHA regulations and with the Standards for Privacy of Individually-Identifiable Health Information (45 CFR Parts 160 and 164). Obtaining and disclosing individually-identifiable patient records must be in compliance with all applicable and confidential statutes and regulations (including those described in the opening two paragraphs of this SOP).

DISCLOSURE TO NON-VHA INVESTIGATORS FOR NON-VA RESEARCH

Persons not employed by VA can be given access to medical and other VA records for R&D purposes only, within the legal restrictions imposed by such laws as the Privacy Act of 1974 and 38 U.S.C. Requests for such use must be submitted to the Chief Research and Development Officer (CRADO) in VA Central Office at least 60 days before access is desired. Requests for information filed pursuant to the Freedom of Information Act ordinarily require a response within 20 working days. VA guidelines and policy must be followed when making such requests to allow for a timely reply. This does not apply to those individuals having access for the purpose of monitoring the research. Obtaining and using the records must be in compliance with all VHA regulations and with the Standards for Privacy of Individually-Identifiable Health Information (45 CFR Parts 160 and 164).

Requests for information filed pursuant to the Freedom of Information Act (FOIA) must be handled in accordance with VA FOIA implementing guidelines. Request pursuant to the FOIA Must be forwarded to the FOIA/Privacy Officer, Chief MAS (136).

TISSUE BANKING

Tissue storage must meet the requirements specified in VHA Directive 2000-043: "Banking of Human Research Subjects Specimens" and the related letter from the Chief Research and Development Officer of March 28, 2001. Specimens stored off-site for future tests not specified in a VA-approved protocol must be only in facilities approved by the VA for tissue banking.

INSTITUTIONAL REVIEW BOARD (IRB) CONSIDERATIONS

Privacy can be defined in terms of having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others. **Confidentiality** pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure without permission. (OHRP IRB Guidebook, Section D. Privacy and Confidentiality)

In accordance with VHA Directive 2007-040, the IRB, which includes the Information Security and Privacy Officers (ISO/PO), will thoroughly review each human subjects research protocol, and will consider the nature, probability, and magnitude of harms that would likely result to the subject from the disclosure of the information collected, prior to research commencement. The IRB shall evaluate the proposed used of PHI. In addition, the IRB will evaluate the proposed coding systems, encryption methods, storage facilities, and access limitations as well as plans for de-identifying data, plans for the final destruction of data at the end of a study, and other relevant factors necessary for determining the adequacy of confidentiality and if applicable anonymity protections. This review process may include the approval of the issue of an encrypted thumb drive to the investigator or staff by the ISO.

Circumstances under which the IRB may consider the provision of privacy protections to be appropriate:

- The data is to be obtained in a setting, with methods and in circumstances that respect an individual's privacy and that is appropriate to the nature of the information being sought.

- The data is to be obtained with informed consent or data to be obtained without informed consent meets the criteria for waiver. *(Researchers ordinarily use information that subjects have disclosed or provided voluntarily for research purposes [*i.e.*, with their informed consent]. Under these circumstances, there is little reason for concern about privacy, other than to assure that appropriate confidentiality of research data is maintained.)* (OHRP IRB Guidebook, Section D. Privacy and Confidentiality)

CERTIFICATES OF CONFIDENTIALITY

Where research involves the collection of highly sensitive information about individually identifiable subjects, the IRB may determine that subjects need to be protected from risks of the investigative or judicial processes. In such situations

the IRB may require that an investigator obtain a Department of Health and Human Services (DHHS) Certificate of Confidentiality (CoC). CoC's are issued by the National Institutes of Health (NIH). Information on obtaining CoC's may be found at the NIH Certificates of Confidentiality Kiosk website (http://grants.nih.gov/grants/policy/coc/index.htm).

For studies with an Investigational New Drug Application (IND) or an Investigational Drug Exemption (IDE), the sponsor can request a CoC from the FDA.

CoC's are issued to protect identifiable research information from forced disclosure. They allow the investigator and others who have access to research records to refuse to disclose identifying information on research participants in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level. CoC's may be granted for studies collecting information that, if disclosed, could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation. By protecting researchers and institutions from being compelled to disclose information that would identify research subjects, CoC's help achieve the research objectives and promote participation in studies by assuring confidentiality and privacy to participants.

The CoC does not prohibit voluntary disclosure of information by an investigator, such as voluntary reporting to local authorities of child abuse or of a communicable disease. In addition, the CoC does not protect against the release of information to VA, DHHS or FDA for audit purposes. Consequently, VAMC designated IRBs shall require that these conditions for release be stated clearly and explicitly in the informed consent document.

REPORTING BREACHES OF CONFIDENTIALITY AND VIOLATIONS OF INFORMATION SECURITY

The IRB ensures that reports of any unauthorized use, loss, or disclosure of individually-identifiable patient information are forwarded to the Privacy Officer (136) per VHA Handbook 1200.5.7.d (12).

The IRB ensures that reports of violations of VA information security requirements are forwarded to the Information Security Officer per VHA Handbook 1200.5.7.d (13).